



Postfix – Dovecot - Debian

Autor: Wiktor Ł.
ver. 1.30
wiktor.vip{at}gmail{dot}com

Wiele ludzi ma problem z zainstalowaniem jakiegoś serwera poczty, więc postanowiłem opisać ten problem. Na necie już krąży jeden z moich opisów, ale postanowiłem napisać nowy o nowo zdobytą wiedzę.

W artykule znajdziecie opis instalacji i konfiguracji postfixa, serwera POP i IMAP(dovecot) oraz autoryzacji SMTP (dovecot). Jako dodatek opisałem także jak zrobić dostęp do nasz poczty przez www (squirrelmail) i monitorować wysyłane i odbierane maile (mailgraph, pflogsumm).

Spis treści:

1. Postfix	2
1.1 Instalacja	2
1.2 Wstępna konfiguracja	2
1.3 Test.....	5
2. Serwer POP3 i IMAP	6
2.1 Instalacja	6
2.2 Konfiguracja	7
2.3 Test.....	8
3. Autoryzacja SMTP.....	11
3.1 Autoryzacja – Dovecot SASL.....	11
3.1.1 Konfiguracja	11
3.1.2 Test autoryzacji.....	13
3.2 Szyfrowanie TLS	14
3.2.1 Instalacja	14
3.3.2 Test TLS.....	15
4. Zarządzanie postfix'em.....	16
4.1 Squirrelmail'a czyli poczta przez WWW	16
5. Monitoring	19
5.1 Mailgraph czyli wykresy.....	19
5.2 Pflogsumm czyli raport.....	20

1. Postfix

Postfix to szybki, łatwy w administracji (w porównaniu z innymi dostępnymi aplikacjami tego typu) i bezpieczny zestaw oprogramowania umożliwiającego stworzenie serwera pocztowego. Zbudowany jest on z wielu mniejszych programów współpracujących ze sobą. Pierwsza zaleta (patrząc od strony bezpieczeństwa) jest fakt, i kolejki FIFO wykorzystywane do komunikacji pomiędzy owymi programami znajdują się w chronionych katalogach.

1.1 Instalacja

Instalacja pakietów podstawowych, niezbędnych do uruchomienia serwera Postfix:

```
Shell
# aptitude install postfix postfix-doc openssl
```

- *postfix* – agent poczty,
- *postfix-doc* – dokumentacja dla postfix'a,
- *openssl* - biblioteka funkcji kryptograficznych i obsługi certyfikatów.

Gdy konfigurator przejdzie do postfixa "Klikamy OK", Następnie wybieramy „No configuration” i OK.

1.2 Wstępna konfiguracja

Tworzymy lub edytujemy plik konfiguracyjny postfixa:

```
Shell
# nano /etc/postfix/main.cf
```

Wklejamy i edytujemy zawartość poniższego konfiga

```
File
command_directory = /usr/sbin
mail_owner = postfix
mydomain = test.com
myhostname = debian

myorigin = /etc/mailname
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

mydestination = $mydomain, $myhostname, localhost, localhost.localdomain,

mynetworks = 127.0.0.0/8
inet_interfaces = all
inet_protocols = ipv4

home_mailbox = Maildir/
mail_spool_directory = /home/

smtpd_banner = ESMTP on $myhostname !
```



```
mailbox_size_limit = 0
recipient_delimiter = +

biff = no
append_dot_mydomain = no
relayhost =
```

A teraz wyjaśnienie opcji:

command_directory	catalog lokalizujący demona
mail_owner	użytkownik pod którym Postfix wykonuje większość operacji
mydomain	nazwa domeny
myhostname	nazwa hosta (tak przedstawia się serwer EHLO)
myorigin	co będzie dodawane po @, gdy brak domeny w adresie z pola from myorigin = \$myhostname ("user@\$myhostname") myorigin = \$mydomain ("user@\$mydomain")
alias_maps alias_database	stosowane bazy aliasów
mydestination	jakiś domeny docelowe (poza wirtualnymi) mają być akceptowane myorigin = \$myhostname ("user@\$myhostname") myorigin = \$mydomain ("user@\$mydomain")
mynetworks mynetworks_style	określenie komputerów, których pocztę będziemy przekazywać mynetworks_style = subnet (z klientów SMTP z naszej podsięci) mynetworks_style = host (tylko z maszyny lokalnej) mynetworks = 127.0.0.0/8 (tylko lokalna maszyna) mynetworks = 127.0.0.0/8 168.100.189.2/32
inet_interfaces	adres interfejsu, na którym będzie nasłuchiwał postfix inet_interfaces = \$myhostname, localhost (nasz host oraz localhost) inet_interfaces = all (wszystkie interfejsy)
inet_protocols	wersja protokołu
home_mailbox	typ skrzynek

mail_spool_directory	katalog z poczta dla skrzynek mailbox
smtpd_banner	sposób przedstawiania się przez serwer
mailbox_size_limit	maksymalny rozmiar skrzynki pocztowej (0 . brak limitu)
recipient_delimiter	niezbędne do monitorowania domen wirtualnych
relayhost =	...
message_size_limit	Maksymalna wielkość wysyłanej wiadomości message_size_limit = 10240000 (10MB)
queue_run_delay maximal_queue_lifetime	Parametry odpowiedzialne za dostarczenie maila jeżeli serwer jest wyłączony (queue_run_delay = 30m maximal_queue_lifetime = 3d sprawdzaj zdalny Server co pół godziny i zwracaj błąd do nadawcy po trzech dniach)
unknown_local_recipient_reject_code	Numer kodu, który będzie zwracany, gdy w systemie nie ma odbiorcy unknown_local_recipient_reject_code = 550
local_destination_concurrency_limit	Ustawia limit ilości wiadomości, które mogą być dostarczone do użytkownika w tym samym czasie
default_destination_concurrency_limit	Ustawia limit ilości użytkowników, których Postfix może obsłużyć równocześnie w tym samym czasie

Sprawdzamy składnię plików konfiguracyjnych:

```
Shell
# postfix check
```

Tworzymy bazę aliasów:

```
Shell
# newaliases
```

Restartujemy demona:



Shell

```
# /etc/init.d/postfix restart
Stopping Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
```

1.3 Test

W tym momencie możemy już sprawdzić, czy nasz daemon SMTP działa. Dokonujemy tego z wykorzystaniem komendy telnet:

Shell

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTP on debian !
EHLO test.com
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Powinniśmy zobaczyć komunikat mniej więcej jak powyżej.

2. Serwer POP3 i IMAP

Postfix jest agentem MTA służącym do nasłuchiwania na porcie 25 i ewentualnie przekazywania odebranej poczty dalej. Aby mieć również możliwość odbierania poczty, dokonamy instalacji serwera POP3 i IMAP. Wykorzystamy do tego zestaw pakietów dovecot.

2.1 Instalacja

```
Shell
# aptitude install dovecot-imapd dovecot-pop3d dovecot-common
```

- *dovecot-common* – dokumentacja dla serwerów POP i IMAP
- *dovecot-imapd* - serwer IMAP wspierający mbox i maildir poczty
- *dovecot-pop3d* - serwer POP3 wspierający mbox i maildir poczty

Ustawmy prawa dla katalogów:

```
Shell
# chmod 755 /var/run/dovecot
# chgrp dovecot /var/run/dovecot/login/
```

Tworzymy katalog w którym będziemy przechowywać nasz certyfikat

```
Shell
# mkdir -p /etc/postfix/ssl
```

Przechodzimy do katalogu

```
Shell
# cd /etc/postfix/ssl
```

Tworzymy certyfikat i podajemy potrzebne dane

```
Shell
# openssl req -new -x509 -nodes -out mail.pem -keyout mail.pem -days 365
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:POLAND
Locality Name (eg, city) []:Warszawa
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moj certyfikat
Organizational Unit Name (eg, section) []:POCZTA
Common Name (eg, YOUR name) []:test.com
Email Address []:root@test.com
```

UWAGA!!! Ważne żeby w polu **Common Name** podać własną domenę

2.2 Konfiguracja

Na początku zrobimy kopie pliku konfiguracyjnego dovecota

```
Shell
# cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.old
```

Edytujemy plik:

```
Shell
# nano /etc/dovecot/dovecot.conf
```

I wklejamy poniższy konfig

```
File
base_dir = /var/run/dovecot/
protocols = imap imaps pop3 pop3s
listen = *
disable_plaintext_auth = no
shutdown_clients = yes

#logi
log_path=/var/log/dovecot.log
info_log_path = /var/log/mail.log
log_timestamp = "%Y-%m-%d %H:%M:%S "
syslog_facility = mail

login_process_size = 64
login_greeting = Welcome. I'm ready ...
login_log_format_elements = user=<%u> method=%m rip=%r lip=%l %c
login_log_format = %$: %s

login_chroot = no
login_user = dovecot
login_process_per_connection = yes
login_processes_count = 3
login_max_processes_count = 128

mail_location = maildir:~/Maildir

#SSL
ssl_disable = no
ssl_cert_file = /etc/postfix/ssl/mail.pem
ssl_key_file = /etc/postfix/ssl/mail.pem
verbose_ssl = yes

mail_access_groups = postfix

protocol imap {
}

protocol pop3 {
    pop3_uidl_format = %08Xu%08Xv
}
```

```
protocol lda {
    postmaster_address = postmaster@test.com
}

auth_verbose = yes
auth_debug = yes

auth default {
    mechanisms = plain login

    passdb pam {
    }
    userdb passwd {
    }
    user = root
}

dict {
}

plugin {
}
```

Startujemy daemona

```
Shell
# /etc/init.d/dovecot start
```

Wszystko powinno być OK, ale jeżeli dovecot nie chce wystartować należy sprawdzić logi.

2.3 Test

Musimy najpierw dodać do systemu dwóch testowych userów np. *nadawca* i *odbiorca* i nadajmy im hasła *haslo* dla obu takie samo.

```
Shell
# useradd -m nadawca
# passwd nadawca
Enter new UNIX password:
. . .
# useradd -m odbiorca
# passwd odbiorca
Enter new UNIX password:
```

Testowanie serwera SMTP:



```
Shell
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTP on debian !
EHLO test.com
250-debian
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: nadawca@test.com
250 2.1.0 Ok
rcpt to: odbiorca@test.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: mail testowy

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
250 2.0.0 Ok: queued as A912CBACD
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Po wysłaniu maila powinien się automatycznie utworzyć katalog Maildir w katalogu domowym usera

```
Shell
# ls -l /home/odbiorca
razem 4
drwx----- 5 odbiorca odbiorca 4096 2007-11-03 15:59 Maildir
```

Testowanie serwera POP3 – nieszyfrowanego:

```
Shell
# telnet localhost 110
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Welcome. I'm ready ...
user odbiorca
+OK
pass haslo
+OK Logged in.
stat
+OK 1 485
list
+OK 1 messages:
1 485
```



```
.
retr 1
+OK 485 octets
Return-Path: <nadawca@test.com>
X-Original-To: odbiorca@test.com
Delivered-To: odbiorca@test.com
Received: from test.com (localhost [127.0.0.1])
        by debian (Postfix) with ESMTP id A912CBACD
        for <odbiorca@test.com>; Sat,  3 Nov 2007 15:54:52 +0100 (CET)
Subject: mail testowy
Message-Id: <20071103145513.A912CBACD@debian>
Date: Sat,  3 Nov 2007 15:54:52 +0100 (CET)
From: nadawca@test.com
To: undisclosed-recipients:;

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
quit
+OK Logging out.
Connection closed by foreign host.
```

Testowanie serwera POP3 – szyfrowanego:

```
Shell
# openssl s_client -connect localhost:995

<tutaj pojawia się informacja dotycząca klucza>
+OK Welcome. I'm ready ...
user odbiorca
+OK
pass hasło
+OK Logged in.
stat
+OK 1 485
retr 1
+OK 485 octets
Return-Path: <nadawca@test.com>
X-Original-To: odbiorca@test.com
Delivered-To: odbiorca@test.com
Received: from test.com (localhost [127.0.0.1])
        by debian (Postfix) with ESMTP id A912CBACD
        for <odbiorca@test.com>; Sat,  3 Nov 2007 15:54:52 +0100 (CET)
Subject: mail testowy
Message-Id: <20071103145513.A912CBACD@debian>
Date: Sat,  3 Nov 2007 15:54:52 +0100 (CET)
From: nadawca@test.com
To: undisclosed-recipients:;

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
quit
+OK Logging out.
read:errno=0
```

3. Autoryzacja SMTP

Kolejnym etapem naszych prac, będzie instalacja autoryzacji poczty wychodzącej SMTP, co zapewni nam nieautoryzowane wykorzystywanie naszego konta pocztowego. Wykorzystamy do tego już zainstalowany Dovecot.

3.1 Autoryzacja – Dovecot SASL

3.1.1 Konfiguracja

Aby włączyć w Dovecot SASL musi dodać odpowiednie wpisy do pliku konfiguracyjnego

```
Shell
# nano /etc/dovecot/dovecot.conf
```

Dodajemy tylko wartości pogrubione reszta już istnieje w pliku

```
File
auth default {
    mechanisms = plain login

    passdb pam {
    }
    userdb passwd {
    }
    user = root

    socket listen {
        client {
            path = /var/spool/postfix/private/auth
            mode = 0660
            user = postfix
            group = postfix
        }
    }
}
```

Aby autoryzacja doszła do skutku należy poinformować o tym Postfiksa, że użytkowników ma autoryzować przez "Dovecot SASL". Dlatego też edytujemy plik:

```
Shell
# nano /etc/postfix/main.cf
```

I dodajemy poniższe wartości

File

```
#AUTH SMTP
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

smtpd_sasl_auth_enable = yes
smtpd_sasl2_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = $myhostname
```

I wyjaśnienie użytych opcji:

- **smtpd_sasl_type** - określamy z jakiej autoryzacji będziemy korzystać.
- **smtpd_sasl_path** - nazwa pliku konfiguracyjnego dla autoryzacji.
- **smtpd_sasl_auth_enable** - uaktywniamy autoryzację SASL
- **smtpd_sasl2_auth_enable** - uaktywniamy autoryzację SASL2
- **smtpd_sasl_security_options** - metody autoryzacji, które nie będą obsługiwane
- **broken_sasl_auth_clients** - zgodność ze starszymi klientami pocztowymi np. OutlookExpress4
- **smtpd_sasl_local_domain** - Ustawienie autoryzacji jest wymagana przy wysyłaniu listów z określonych tutaj domen. Jeśli zostawisz ten parametr pusty będzie to oznaczało, że autoryzacja jest wymagana przy wszystkich domenach na Twoim serwerze

Wprowadźmy jeszcze kilka zabezpieczeń przez spamem na poziomie postfixa

Shell

```
# nano /etc/postfix/main.cf
```

I dodajemy poniższe wartości

File

```
smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination,
    reject_unknown_recipient_domain,
    reject_non_fqdn_recipient

smtpd_client_restrictions =
    permit_sasl_authenticated,
    #reject_unknown_client,
    reject_rbl_client dul.dnsbl.sorbs.net,
    reject_rbl_client list.dsbl.org,
    reject_rbl_client sbl.spamhaus.org,
    reject_rbl_client cbl.abuseat.org

smtpd_sender_restrictions =
    permit_sasl_authenticated,
    reject_unknown_sender_domain,
    reject_non_fqdn_sender,
    reject_unknown_address
```

smtp_recipient_restrictions - sprawdzanie poczty na podstawie adresu nadawcy listu (RCPT TO)

- **permit_mynetworks** - pozwala na połączenie się z naszym serwerem komputerom, z naszej sieci lokalnej (dokładnie: komputerom, które zostały ujęte w zmiennej \$mynetworks)
- **permit_sasl_authenticated** - pozwala na połączenia z autoryzacją.
- **reject_unauth_destination** - odrzuć list, jeśli to nasz serwer nie jest jego przeznaczeniem. Odrzuca list, nie sprawdza innych ograniczeń.
- **reject_unknown_recipient_domain** - odrzuć, jeśli adres docelowy listu, jego adres nie istnieje w DNS (czyli i tak nie ma dokąd go wysłać)
- **reject_non_fqdn_recipient** - odrzuć list, jeśli podany adres odbiorcy nie jest "pełny" (fully-qualified domain form)

smtpd_client_restrictions - Restrykcje - Sprawdzenie IP komputera, z którego wysyłana jest wiadomość

- **permit_mynetworks** - pozwala na połączenie się z naszym serwerem komputerom, z naszej sieci lokalnej (dokładnie: komputerom, które zostały ujęte w zmiennej \$mynetworks)
- **reject_unknown_client** - odrzuca komputer, którego adresu IP nie ma w DNS
- **reject_rbl_client** - RLB bazy adresów spamatorów

smtpd_sender_restrictions - Restrykcje - Sprawdzanie poczty na podstawie adresu odbiorcy listu (MAIL FROM) nadawcy listu (RCPT TO)

- **permit_sasl_authenticated** - pozwala na połączenia z autoryzacją.
- **reject_unknown_sender_domain** - odrzuca list, jeśli adres nadawcy, dokładnie część po @ adresu nadawcy, nie ma wpisu w DNS.
- **reject_non_fqdn_sender** - odrzuć list, jeśli podany adres odbiorcy nie jest "pełny" (fully-qualified domain form)

Dokładniejszy opis wszystkich opcji na stronie: http://lemat.priv.pl/index.php?m=page&pg_id=90

Restartujemy dovecota i postfixa

```
Shell
# /etc/init.d/dovecot restart
# /etc/init.d/postfix restart
```

3.1.2 Test autoryzacji

Sprawdzamy czy działa

```
Shell
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTP on debian !
EHLO test.com
```

```
250-debian
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Jeżeli są te dwie linijki które są podkreślone to znaczy że wszystko działa.

3.2 Szyfrowanie TLS

3.2.1 Instalacja

Znow edytujemy



```
# nano /etc/postfix/main.cf
```

I dodajemy poniższe wartości do pliku:



```
#TLS
smtpd_tls_auth_only = yes
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/mail.pem
smtpd_tls_cert_file = /etc/postfix/ssl/mail.pem
smtpd_tls_CAfile = /etc/postfix/ssl/mail.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache
tls_random_source = dev:/dev/urandom
```

I wyjaśnienie użytych opcji:

- **smtpd_tls_auth_only** - autoryzacja odbywa się jedynie poprzez szyfrowanie
- **smtp_use_tls** - parametry uaktywniające używanie TLS dla SMTP
- **smtpd_use_tls** - parametry uaktywniające używanie TLS dla SMTPD
- **broken_sasl_auth_clients** - połączenia (poprzez tunele TLS)
- **smtpd_tls_key_file** - ścieżka do pliku zawierający wygenerowany klucz dla SMTP
- **smtpd_tls_cert_file** - ścieżka do pliku zawierający wygenerowany certyfikat dla SMTP
- **smtpd_tls_CAfile** - ścieżka do pliku zawierający wygenerowany certyfikat dla SMTP
- **smtpd_tls_loglevel** - informacja diagnostyczna
- **smtpd_tls_received_header** - Sprawdzenie, czy informacje dotyczące protokołu oraz szyfru zawarte są w nagłówku wiadomości
- **smtpd_tls_session_cache_timeout** - czas wygasania sesji TLS
- **tls_random_source** - źródło losowości

Gdy już wszystko mamy:

```
Shell
# /etc/init.d/postfix restart
```

3.3.2 Test TLS

Sprawdzamy czy działa

```
Shell
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTP on debian !
EHLO test.com
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Zauważ, że poniższe dwie linijki, które były aktywne w czasie gdy konfigurowaliśmy SMTP AUTH, mówię tu o:

```
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
```

zastąpiła jedna:

```
250-STARTTLS
```

Jeśli ukazał Ci się taki komunikat, wszystko działa OK. Jeżeli jednak chcesz zobaczyć te dwie dodatkowe linie zmień: w pliku `main.cf` wartość: `smtpd_tls_auth_only = yes` na `no`

4. Zarządzanie postfix'em

4.1 Squirrelmail'a czyli poczta przez WWW

Na koniec przydało by się zrobić użytkownika poczty dostęp przez WWW, a do tego najlepiej nadaje się squirrelmail, więc zainstalujemy go.

```
Shell
# aptitude install squirrelmail squirrelmail-locales
```

- *squirrelmail* – umożliwia dostęp do poczty przez www,
- *squirrelmail-locales* – paczka językowa do squirrelmail'a,

Po zainstalowaniu robimy symboliczne dowiązanie pliku apache.conf

```
Shell
# ln -s /etc/squirrelmail/apache.conf /etc/apache2/conf.d/squirrelmail
```

I edytujemy plik:

```
Shell
# nano /etc/squirrelmail/apache.conf
```

Na samym początku tego pliku znajdujemy ta wartość:

```
File
Alias /squirrelmail /usr/share/squirrelmail
```

I zmieniamy jak poniżej

```
File
Alias /poczta /usr/share/squirrelmail
```

Zróbmy jeszcze dowiązanie do plików squirrelmail w katalogu WWW, żeby łatwiej było znaleźć:

```
Shell
# ln -s /usr/share/squirrelmail /var/www/poczta
```




Teraz reset apache:

```
Shell
# /etc/init.d/apache2 restart
```

I sprawdzamy czy wszystko działa wpisując poniższy adres w przeglądarce (działa tylko na localhostie):

<http://localhost/poczta/src/configtest.php>

Powinieneś zobaczyć kilka komunikatów takich jak:

```
File
Checking PHP configuration...
  PHP version 5.2.0-8+etch7 OK.
  PHP extensions OK.
Checking paths...
  Data dir OK.
  Attachment dir OK.
  Plugins are not enabled in config.
  Themes OK.
  Default language OK.
  Base URL detected as: http://localhost/poczta/src (location base autodetected)
Checking outgoing mail service....
  SMTP server OK (220 ESMTP on debian !)
Checking IMAP service....
  IMAP server ready (* OK Welcome. I.m ready ...)
  Capabilities: * CAPABILITY IMAP4rev1 SASL-IR SORT THREAD=REFERENCES MULTIAPPEND
UNSELECT LITERAL+ IDLE CHILDREN NAMESPACE LOGIN-REFERRALS STARTTLS AUTH=PLAIN
AUTH=LOGIN
Checking internationalization (i18n) settings...
  gettext - Gettext functions are available. You must have appropriate system
locales compiled.
  mbstring - Mbstring functions are available.
  recode - Recode functions are unavailable.
  iconv - Iconv functions are available.
  timezone - Webmail users can change their time zone settings.
Checking database functions...
  not using database functionality.

Congratulations, your SquirrelMail setup looks fine to me!
```

Ustawmy jeszcze w squirrelmaila nasz predefiniowany serwer IMAP czyli devecot, w tym celu wykonaj polecenie:

```
Shell
# /usr/sbin/squirrelmail-configure
```

Po uruchomieniu tego skryptu zobaczysz takie “okno” jak poniżej

```
Shell
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C  Turn color on
S  Save data
Q  Quit

Command >>
```

Wpisujemy **D** i wciskamy Enter

```
Shell
SquirrelMail Configuration : Read: config.php
-----
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
  bincimap      = Binc IMAP server
  courier       = Courier IMAP server
  cyrus         = Cyrus IMAP server
  dovecot       = Dovecot Secure IMAP server
  exchange     = Microsoft Exchange IMAP server
  hmailserver   = hMailServer
  macosx        = Mac OS X Mailserver
  mercury32     = Mercury/32
  uw           = University of Washington's IMAP server

  quit         = Do not change anything
Command >> dovecot
```

Teraz tylko wpisujemy z jakiego serwera IMAP korzystamy i Enter, w następnym okienku zostaw wszystko domyślnie. Zapisz ustawienia i wyjdź z konfiguratora.

5. Monitoring

5.1 Mailgraph czyli wykresy

Mailgraph tworzy dzienne, tygodniowe, miesięczne i roczne wykresy z wysłanych odebranych, bounced i odrzuconych wiadomości także spamu i wirusów jeżeli SpamAssassin i ClamAV jest zintegrowany z Postfixem.

```
Shell
# aptitude install rrdtool mailgraph
```

- *rrdtool* - Time-series data storage and display system (programs),
- *mailgraph* - Mail statistics RRDtool frontend for Postfix

Podczas instalacji będziesz pytany o kilka rzecz zaznacz jak poniżej: (Jeżeli masz zintegrowanego z Postfix'em amavis'a do filtrowania spamu i wirusów wtedy w opcji *Count incoming mail as outgoing mail?* zaznacz *No* żeby uniknąć podwójnego liczenia maili (ponieważ Postfixa dostarcza maile do amavis'a który po dokonaniu skanowania odsyła je z powrotem do Postfix'a). Jeżeli nie używasz żadnego skanera wtedy możesz zaznaczyć *Yes*)

Jeżeli instalator nie zapytał cię o te opcje podaj wydaj polecenie *dpkg-reconfigure mailgraph*

```
File
Should Mailgraph start on boot?          <-- Yes
Which logfile should be used by mailgraph? <-- /var/log/mail.log
Count incoming mail as outgoing mail?    <-- Yes
```

Utwórz katalog

```
Shell
# mkdir -p /var/www/cgi-bin/
```

Zrób link symboliczny do skryptów odpowiedzialnych za generowanie wykresów

```
Shell
# ln -s /usr/lib/cgi-bin/mailgraph.cgi /var/www/cgi-bin/
```

Żeby zobaczyć nasze wykresy wpisujemy w przeglądarce:

<http://localhost/cgi-bin/mailgraph.cgi>

5.2 Pflogsumm czyli raport

Pflogsumm jest skryptem napisanym w perlu do generowania statystyk z logów maila. Mamy takie statystyki jak: z którego konta zostało wysłano najwięcej maili, kto do nas wysłał najwięcej maili, w których godzinach jest wysyłane najwięcej mail itd. ...

Przedstawię tu jak zainstalować i skonfigurować ten skrypt żeby otrzymywać raz w tygodniu raport z wysłanych i otrzymanych mail.

Zainstalujemy ten skrypcik:

```
Shell
# aptitude install pflogsumm mutt
```

- *pflogsumm* - Postfix log entry summarizer
- *mutt* - text-based mailreader supporting MIME, GPG, PGP and threading

Zanim zajmiemy się konfiguracją skryptu najpierw musimy skonfigurować, aby logi mail były pakowane raz dziennie w tym celu tworzymy plik:

```
Shell
# nano /etc/logrotate.d/mail
```

I dodajemy poniższą zawartość

```
File
/var/log/mail.log {
    missingok
    daily
    rotate 7
    create
    compress
    start 0
}
```

Tworzymy plik:

```
Shell
# nano /root/bin/postfix_report.sh
```

Dodajemy poniższą zawartość i zmieniamy odpowiednie wartości:



File

```
#!/bin/bash

EMAILS="qqq@test.com xxx@test.pl"
SUBJECT="Statystyki mail z `hostname`"

gunzip /var/log/mail.log.0.gz
pflogsumm /var/log/mail.log.0 | mutt -s "$SUBJECT" $EMAILS
gzip /var/log/mail.log.0
exit 0
```

Nadajmy prawa do wykonywania dla tego pliku:

Shell

```
# chmod 750 /root/bin/postfix_report.sh
```

Otwórzmy plik cron'a:

Shell

```
# nano /etc/crontab
```

Dodajmy go do crona aby wykonywał się codziennie o 7:00 i wysyłał nam raport na podany przez nasz adres w skrypcie.

File

```
0 7 * * * /root/bin/postfix_report.sh &> /dev/null
```